

CLAIMS

What is claimed is:

1. A device for preventing the unauthorized use of proprietary data, the apparatus comprising:
 - a user authentication device configured to provide the user an authentication data input for proving the user is authorized to use the account number;
 - a transaction counting mechanism configured to track authorized device access events;
 - a processor device in electrical communication with the user authenticator and counter, the processor being programmed to generate a security key in response to authentication data received via the user authenticator, the security key being derived at least in part from the contents of the counter; and
 - a display unit configured to display the security key on the apparatus.
2. The device of Claim 1, wherein the security key is derived from the contents of the counter and a user's PIN.
3. The device of Claim 2, wherein the security key is encrypted before being displayed.
4. The device of Claim 2, further comprising a wireless transmitter to transmit the security key to a network device.
5. The device of Claim 4, further comprising a smart card reader, wherein the apparatus can be used with existing smart cards to provide a security key for transactions.

6. The device of Claim 2, wherein the apparatus is connected to a computer to authorize transactions on a network.

7. The device of Claim 2, wherein the user authenticator is a PIN entry system.

8. The device of Claim 1, further comprising a clocking mechanism having an output coupled to the processor device, wherein said processing device also uses the clocking mechanism output to derive the security key.

9. A system for securely processing transactions, the system comprising:

a security key device, comprising,

a user authenticator configured to provide a user an authentication data input for proving the user is authorized to use an account associated with the security device,

a first counter in communication with the user authenticator,

a key generator in communication with the user authenticator and first counter, the key generator being programmed to generate a security key in response to authentication data received via the user authenticator, the security key being derived at least in part from contents of the first counter, and

an electronic display in electrical communication with the key generator, for displaying the security key in a manner visible upon the structure; and

an authorization device, comprising,

a second counter, and

a key confirmation processor programmed to confirm an authenticity of the security key in a manner at least partially dependent upon the contents of the second counter.

10. The system of Claim 9, wherein the security key is derived at least partially from the contents of the first counter.

11. The system of Claim 9, wherein the security key is derived at least partially from the contents of the first counter and a user PIN.

12. The system of Claim 10, wherein the key confirmation processor approves a transaction if the contents of the first counter matches contents of the second counter within a predetermined range.

13. The system of Claim 10, wherein the security key is encrypted before being displayed and the key confirmation processor decrypts the key in order to authenticate a transaction.

14. The system according to Claim 9, wherein:
the security key device further comprises a first clocking mechanism having an output coupled to the key generator, and the key generator programming includes use of the clocking mechanism output to generate the security key;
the authorization device further comprises a second clocking mechanism synchronized to the first clocking mechanism, and a second counter; and

the key confirmation processor is programmed to confirm an authenticity of the key in a manner at least partially dependent upon the contents of the second counter and an output of the second clocking mechanism.

15. The device according to Claim 14, wherein the clocking mechanisms are based on a time variant device.

16. The device according to Claim 14, wherein said clocking mechanisms are based on actual time.

17. The device according to Claim 9, wherein the authorization device is configured to retrieve the security key from a PIN field of a received transaction communication.

18. A method of securely authorizing a transaction utilizing an account, the method comprising:

confirming an authorized use of an account card via a PIN provided by a user;

maintaining a first count indicative of a number of instances of such authorized uses;

generating a security key in a manner at least partially dependent upon the count;

transmitting the security key to an authorizing authority;

processing the security key at the authorizing authority;

maintaining a second count indicative of a number of transmissions received by the authorizing authority for the account;

confirming that the security key was generated by an authorized user at least in part through use of the second count; and

authorizing the transaction if the security key was generated by an authorized user.

19. The method of Claim 18, wherein the PIN is input by a keypad.

20. The method of Claim 18, wherein the security key is generated using an encryption algorithm to process a card key and the first count.

21. The method of Claim 20, wherein the transaction is authorized if the first count is within a predefined number of the second count.

22. The method of Claim 21, wherein the card key is generated from a master key provided by the account provider and from a user's bio-metric data.

23. The method according to Claim 21, further comprising the step of:
maintaining first and second clocking devices configured to respectively produce first and second clock signals;

wherein:

said step of generating a security key comprises generating a security key in a manner at least partially dependent upon the count and the first clocking device; and

said step of confirming the security key comprises confirming that the security key was generated by an authorized user at least in part through use of the second count and the second clock signal.

24. The method of Claim 18, wherein said step of transmitting the security key comprises transmitting the security key in a PIN field of a transaction communication to the authorizing authority.

25. A smart card, comprising,

an activation device configured to produce a signal in response to a user action;

a display mechanism;

wherein:

said programming is further configured to,

retrieve a bio-metric input from said bio-metric sensing device and compare the bio-metric input to a stored bio-metric value prior to one of calculating and displaying the encrypted key, and

verify said user action prior to displaying the encrypted key prior to one of calculating and displaying the encrypted key; and

if said comparison of the bio-metric input does not match the bio-metric value, or, if the user action is not verified, then, displaying one of an error message and a non-authentic value instead of the encrypted key.

33. The smart card according to Claim 32, wherein said bio-metric sensing device is a fingerprint scanner.

34. The smart card according to Claim 25, further comprising:

a clocking mechanism configured to produce a time variant clock value;

wherein said programming is further configured to utilize the clock value in producing the encrypted key.

35. The smart card according to Claim 34, further comprising:

a transaction counter configured to produce a transaction count based on a number of transactions performed utilizing the smart card;

wherein said programming is further configured to utilize the transaction count in producing the encrypted key.

36. A smart card, comprising,

an activation device configured to produce a signal in response to a user action;

a display mechanism;

a processing device coupled to the display device and configured to receive said signal;

and

programming executable by the processing device upon receipt of said signal and configured to produce an encrypted key and display the encrypted key on the display mechanism;

wherein:

said smart card comprises a credit card sized enclosure;

said display mechanism is disposed on a face of the credit card sized enclosure;

said programming is stored on a computer readable media disposed on or within the credit card sized enclosure;

said credit card sized enclosure in a solid flexible material;

said activation device is a numeric entry system disposed on a face of the credit card sized enclosure;

said numeric entry system includes a ten key type entry system and said user action is entry of a PIN via the numeric entry system;

said programming is further configured to verify said user action prior to displaying the encrypted key;

if said programming is unable to verify said user action, then, displaying one of an error message and a non-authentic value on the display mechanism;

said smart card further comprises a bio-metric sensing device coupled to said processing device;

said programming is further configured to retrieve a bio-metric input from said bio-metric sensing device and compare the bio-metric input to a stored bio-metric value prior to one of calculating and displaying the encrypted key,

said bio-metric sensing device is a fingerprint scanner;

said smart card further comprises a transaction counter configured to track authorized transactions associated with the smart card and a clocking mechanism configured to produce a time varying clock value;

said encrypted key is derived, at least in part, based on the transaction counter and time varying clock value; and

said smart card is capable of communicating with an authorization device that, retrieves the encrypted key from a PIN field of a transaction communication,

decrypts the encrypted key using a count from a second transaction counter and a second time varying clock value from a second clocking mechanism synchronized with the first clocking mechanism, and

authorizes a transaction if the decrypted key is valid;

the decrypted key being valid if produced by the smart card with a valid PIN and the first and second transaction counters are synchronized within a predetermined number of transactions.

10040456 134901